UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	Case No. 25-MR-70
19 DUSTY HILL ROAD MESITA, NEW MEXICO, 87026, THE PERSON OF RICKIE SPEAKMAN, YOB 1956	

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, incorporated herein by reference.

located in the District of New Mexico, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2251 – Sexual Exploitation of Children	

The application is based on these facts:

See attached Affidavit, submitted by SA Barragan and approved by Supervisory AUSA Alexander Flores.

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:_____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Barragan, Adam Kyle, FBI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephonically sworn and electronically signed *(specify reliable electronic means).*

Date: 1/15/2025

Judge's signature

City and state: Albuquerque, New Mexico

Steven C. Yarbrough, United States Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF: 19 DUSTY HILL ROAD MESITA, NEW MEXICO, 87026, THE PERSON OF RICKIE SPEAKMAN, YOB 1956	Case No. **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Adam Kyle Barragan, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 19 Dusty Hill Rd., Mesita, New Mexico 87026, (hereinafter referred to as the "Subject Premises"). A more detailed description and photographs of the Subject Premises are contained within "Attachment A," which has been attached hereto and incorporated herein by reference.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since December 2022. As such, I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), and I am empowered by law to conduct investigations and to make arrests for criminal offenses, to include those enumerated in 18 U.S.C. § 2516. I am assigned to the FBI's Albuquerque Field Office and currently assigned to the FBI's Violent Crime Task Force, a joint federal and local task force investigating violations of federal law involving violent criminal offenses committed in the Albuquerque area as well as Indian County offenses, such as homicide, assault, sexual assault, and the sexual abuse and exploitation of children. I have received training in interviewing and interrogation techniques, arrest procedures, search and seizure, search-warrant applications, conducting physical surveillance, consensual monitoring, and electronic and physical surveillance procedures at the

Federal Bureau of Investigation Academy in Quantico, Virginia. I have received on-the-job training from other agents in the investigation of federal offenses, to include interference with federally protected activities and using and carrying a firearm during and in relation to a crime of violence. My investigative training and experience includes, but is not limited to, interviewing subjects, victims, and witnesses, and collecting evidence—including collecting and exploiting electronic devices for evidence of crimes.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement agents, agencies, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2251 – Sexual Exploitation of Children have been violated by one (1) or more of the occupants of the Subject Premises. There is also probable cause to search the information described in Attachments A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachments B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States for the District of New Mexico that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). As discussed more fully below, acts or omissions in furtherance of the offenses under investigation occurred within the state of New Mexico.

DEFINITIONS

6. The following terms are relevant to this affidavit in support of this application for a search warrant:

a. *Child Pornography*: The term "child pornography" is defined at 18 U.S.C. § 2256(8). It consists of visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct, as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct. *See* 18 U.S.C. §§ 2252 & 2256(2), (8).

b. *Computer*: The term "computer" refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

c. *Internet*: The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. *Internet Protocol ("IP") Address*: An IP address is a unique number used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed

properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic", meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static", if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

e. *Minor:* The term "minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

f. *Sexually Explicit Conduct:* The term "sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

g. *Visual Depictions:* "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

h. *Smartphone*: A "smartphone" is a type of mobile or cellular telephone, and functions as multi-purpose mobile-computing devices. Smartphones can function as traditional telephones with the additional ability to store contact information, send and receive voice, text, and media messages, store information and media, access the Internet, and perform many of the same functions as a traditional computer. A smartphone user may perform these various functions through software applications ("apps") which may store evidence of such use on the device.

BACKGROUND ON CHILD EXPLOITATION OFFENSES AND OFFENDER CHARACTERISTICS

7. Based on conversations with other agents and law enforcement officers and my experience in the investigation of computer-related crimes and child exploitation offenses, I know the following:

a. Computers and computer technology, including cellular phones, have revolutionized how sexually explicit material depicting minors is obtained, solicited, produced, distributed, and utilized. In general, computers, including cellular phones, serve four functions in connection with child exploitation offenses: communication, production, distribution/receipt, and storage.

b. Persons engaged in child exploitation offenses most often use the Internet to do so. The Internet offers several different venues for obtaining, viewing, and trading sexually explicit images in a relatively secure and anonymous fashion. Individuals who use the Internet can communicate electronically by using e-mail and other chat or messaging services. E-mail messages can contain text, data, and images. This type of communication is private in that it is directed from one Internet user to another. Internet users can also communicate using chat rooms and instant messaging. Both chat rooms and instant messaging incorporate "real time" communication between Internet users. Instant messaging, like e-mail, is private, in that it is one Internet user communicating specifically, and exclusively, with another. Instant messaging may also occur with more than one person at a time. Internet Service Providers and web sites provide software and venue for such contact. The Internet offers a number of facilities, which allow users to access, distribute, and exchange information including the World Wide Web ("WWW"), File Transfer Protocol

("FTP"), electronic e-mail ("E-mail"), and postings on boards or newsgroups. The WWW allows users to display and access data in a multimedia format.

c. Once persons engaged in child exploitation offenses obtain child pornography material from the Internet, as described above, they often maintain or store this material because the material is valuable to them. Offenders maintain or store child pornography material in a variety of ways. For instance, such persons may store child pornography material on computers, including smartphones, mobile phones and devices, storage devices (including USB drives) and tablets.

d. Persons engaged in child exploitation offenses often use online resources to meet and communicate with other like-minded individuals. The Internet affords such persons several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

e. Persons engaged in child exploitation offenses often use online resources to meet and communicate with minors. Such individuals may receive sexual gratification, stimulation, and satisfaction from virtual contact with children. Such contact often includes conversations that are sexual in nature, requesting sexually explicit conduct from the child, or sending the child sexually explicit images to lower the inhibitions of children. Such persons often use online resources to meet and communicate with multiple minors at any given time.

f. Electronic devices of various types – to include cellular phones, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices, which plug into a port on the computer – can store thousands of images and/or videos at very high resolution. It is extremely easy for an

individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Individuals can easily store, carry, or conceal media storage devices on their persons. Individuals also often carry smartphones and/or mobile phones on their persons.[1]

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

8. Based on my knowledge, experience, and communications with other agents and law enforcement officers, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

9. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

[1] *See United States v. Carpenter*, 138 S. Ct. 2206, 2218 (2018) (noting that individuals "compulsively carry cell phones with them all the time."); *see also Riley v. California*, 134 S. Ct. 2473, 2490 (2014) (referencing a poll finding that "nearly three-quarters of smart phone users report being within five feet of their phones most of the time…").

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to produce and/or elicit child pornography, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my knowledge and experience, I believe that an electronic device used to

commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

10. *Nature of examination*. Based on the foregoing, and consistent with Rule 41 (e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

11. *Location of examination*. Because data on electronic devices may be particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted. Further, the examination may employ techniques that would damage or destroy the device, but result in a forensically sound copy of data stored on the device.

PROBABLE CAUSE

12. The United States, including the FBI, is conducting a criminal investigation of Rickie SPEAKMAN, Year of Birth ("YOB") 1956 and Corey SAKIESTEWA, YOB 2010, a member of the Pueblo of Laguna, regarding a possible violation of 18 U.S.C. § 2251 – Sexual Exploitation of Children.

13. The following section outlines the probable cause and facts surrounding the investigation highlighting why the affiant is requesting a search warrant for the Subject Premises where SPEAKMAN lives, and that was previously shared by SPEAKMAN and SAKIESTEWA. The investigation initiated with two (2) separate investigations, one (1) regarding SPEAKMAN and possible sexual abuse of a minor and a second investigation

regarding SAKIESTEWA and possible sexual exploitation of children. SPEAKMAN was the foster guardian of SAKIESTEWA up to approximately December 2024. SAKIESTEWA's mother was reestablished as the guardian for SAKIESTEWA and SAKIESTEWA returned to his mother's address at 9619 Mirasol Ave. NW, Albuquerque, NM 87120 sometime during or after December 2024.

14. Based on the facts gathered there is probable cause to believe that child pornography is or was at the Subject Premises and either SPEAKMAN and/or SAKIESTEWA solicited said material. This search warrant is also being submitted in conjunction with a separate search warrant for the current residence of SAKIESTEWA at 9619 Mirasol Ave. NW, Albuquerque, NM 87120. Based on my training and experience there is probable cause to believe child pornography or evidence of where the material was solicited or sent can be located at the Subject Premises.

Investigation Regarding SAKIESTEWA

15. On November 19, 2024, the affiant received information from the Pueblo of Laguna Tribal Police Department advising that an unknown subject communicated with several children on the Pueblo of Laguna via Snapchat. The unknown subject enticed a nude picture from J.H., YOB 2012, a member of the Pueblo of Laguna, hereinafter referred to as "Jane Doe 1." Jane Doe 1 informed the Pueblo of Laguna Police Department that she took a full body nude photograph and sent it to the unknown subject over Snapchat. The affiant was informed by the Pueblo of Laguna Police Department that Jane Doe 1 sent the photograph to the Snapchat username "platonicmitch," hereinafter referred to as the "Target Account." Jane Doe 1 stated she sent the photo about one (1) or two (2) weeks prior to November 19, 2024.

16. During the course of the preliminary investigation the Pueblo of Laguna Police Department identified at least two (2) additional children who had contact with the Target Account via Snapchat. One (1) of the individuals was D.C., YOB 2013, a member of the Pueblo

of Laguna, hereinafter referred to as "Jane Doe 2." Jane Doe 2 stated she did not provide any photos to the Target Account. The second individual was SAKIESTEWA. Jane Doe 1 stated SAKIESTEWA was the first person to have contact with the Target Account via Snapchat but does not know how SAKIESTEWA contacted the Target Account.

17. On November 19, 2024, the Pueblo of Laguna Police Department interviewed SAKIESTEWA who stated the Target Account friended him on November 15, 2024. SAKIESTEWA does not know the person, but he asked SAKIESTEWA to have one (1) of his friends add him back on Snapchat. SAKIESTEWA did not speak with the person regarding anything further. SAKIESTEWA was not aware of any rumors that were going on at school.

18. On November 20, 2024, the Pueblo of Laguna Police Department reinterviewed SAKIESTEWA because he advised he had additional information. SAKIESTEWA advised he did not initially tell the investigator all the information because he was scared because he did not want to be blamed for something he did not do. SAKIESTEWA stated on November 16, 2024, the Target Account texted SAKIESTEWA asking if he could add Jane Doe 1 back as a friend. SAKIESTEWA did not know if Jane Doe 1 was friends with the Target Account previously. The Target Account told SAKIESTEWA that he wanted to get something from her but never articulated what it was he wanted to get. SAKIESTEWA had to relay the message through another friend to Jane Doe 1 because he did not have Jane Doe 1's direct Snapchat information. SAKIESTEWA stated the conversations were deleted by Snapchat. During this interview SAKIESTEWA knew that Jane Doe 1 had sent a photo to someone due to rumors at school.

19. The Pueblo of Laguna Police Department received Jane Doe 1, Jane Doe 2, and SAKIESTEWA's phones during their investigation under the assumption that all three (3) individuals were victims in the incident. Consent was provided for all phones for a complete search and the phones were transferred to FBI custody for examination. The affiant conducted

the examination of the phones at the FBI Albuquerque Field Office. During the examination of Jane Doe 1's phone the affiant did not locate any photographs that represent child pornography. The affiant also conducted a search of SAKIESTEWA's phone and did not identify any photographs representing child pornography. The Snapchat account identified on the phone had a username of "juzosuzuya" which is not the same as the Target Account. This was also confirmed during the interview with SAKIESTEWA.

20. Based on the above information the affiant subpoenaed Snapchat regarding the user information associated with the Target Account. The information returned from Snapchat indicated the Target Account was created on November 15, 2024, which would fit the timeline for when Jane Doe 1 sent the photograph. Based on the information received from Snapchat, the email account associated with the Target Account was coreysakiestewa@gmail.com and the associated IP address was 137.118.82.103. The email account name matches the name of SAKIESTEWA. The affiant knows from training and experience a Gmail account can be created with a false name.

21. On December 3, 2024, the affiant had FBI personnel utilize internal database checks to check the location of the Target Account's IP address. It was determined the IP address was utilized by the Pueblo of Laguna. With the assistance of K'awaika Hanu Internet, a local internet service provider, it was confirmed the IP address is part of their network pool and is associated with SPEAKMAN at the Subject Premises. As of December 5, 2024, the IP address was still in use by SPEAKMAN via his router and had been used by SPEAKMAN for approximately one (1) year. This would put the IP address used to create the Target Account at the Subject Premises during the time of the solicitation and the time of the creation of the Target Account. A list of electronic devices connected to SPEAKMAN's router was also provided by K'awaika Hanu Internet which indicated there was a desktop computer attached to the router and another unknown device. This would indicate there are additional electronic

devices that are or were located at the Subject Premises that could store evidence or could have been used to contact Jane Doe 1. One or more of those devices may have been accessed or exclusively used by SAKIESTEWA while he still lived in the Subject Premises.

22. On January 9, 2025, the Affiant was informed that SAKIESTEWA returned to his mother's residence at 9619 Mirasol Ave. NW, Albuquerque, NM 87120.

23. Based on the facts provided; SAKIESTEWA was the first individual identified to have contact with the Target Account, the Target Account was created with an email address under the name of SAKIESTEWA, the IP address associated with the Target Account was utilized by SPEAKMAN and/or an individual using the router at the Subject Premises during the time of the incident, SAKIESTEWA was the foster child of SPEAKMAN during the time of this incident, and SAKIESTEWA lived at the same address as SPEAKMAN, the Subject Premises, during the time. These facts establish probable cause to believe the owner and creator of the Target Account is SAKIESTEWA who currently lives at 9619 Mirasol Ave. NW Albuquerque NM 87120. Based on training and experience and the reasonableness that there are additional electronic devises located at the Subject Premises there is probable cause to believe there will be evidence connecting SAKIESTEWA or SPEAKMAN to the associated crimes.

Investigation Regarding SPEAKMAN

24. On September 2, 2024, the affiant received information from the Pueblo of Laguna Police Department regarding a Children, Youth, and Families Department (CYFD) notification outlining a possible sexual abuse of a minor case that originated out of Virginia. According to the CYFD notification SPEAKMAN was accused of instructing I.D., YOB 2011, hereinafter referred to as "Jane Doe 3," to touch his genitals. The abuse occurred approximately seven (7) years prior to the disclosure and occurred on the Pueblo of Laguna.

25. The affiant contacted the reporting individual from Virginia who is a mental health professional at the Barry Robinson Center in Norfolk Virginia. Jane Doe 3 disclosed to the reporting party that her grandfather, SPEAKMAN, had her touch his genitals at his house in New Mexico. There were no witnesses to the abuse and the abuse occurred when the grandmother was at work. The reporting party stated Jane Doe 3 was at the facility for mental health disorders and tendencies. Jane Doe 3's parents live in North Carolina and Jane Doe 3 would remain at the facility until December 2024.

26. The affiant spoke with Jane Doe 3's father over the phone, who stated there have been integrity issues and accusations which were some of the reasons why she was in the facility. He believed Jane Doe 3 has been sexually abused but does not know by whom or how. The father based his statement on his feelings and an unknown statement Jane Doe 3 had made to him in the past. He stated he is Jane Doe 3's biological father and he is not native American. Jane Doe 3's biological mother was Native American from the Pueblo of Laguna, and she is deceased. SPEAKMAN is the grandfather to Jane Doe 3 via the mother's side.

27. During the time of the investigation two (2) minors were identified as living with SPEAKMAN, SAKIESTEWA and D.B., YOB 2014, hereinafter referred to as "Witness 1." SAKIESTEWA and Witness 1 both were forensically interviewed and neither of the minors disclosed any child abuse by SPEAKMAN.

28. On November 8, 2024, a forensic interview was conducted with Jane Doe 3 who stated she was approximately six (6) or seven (7) years old when SPEAKMAN would touch her. Jane Doe 3 stated she "consented" to this and would do "it" back. The abuse happened when Jane Doe 3 lived in New Mexico and her grandma worked the night shift. Jane Doe 3 did not have a bed at the house, and she would sleep in the bed with SPEAKMAN. Jane Doe 3 stated she could not recall if she "started it." SPEAKMAN would slip his hand in Jane Doe 3's pants and touch her vagina. Jane Doe 3 would then touch SPEAKMAN back. One (1) specific

time Jane Doe 3 recalled she and SPEAKMAN stayed in a hotel together and when they were in bed she felt him against her butt. Jane Doe 3 stated she would touch SPEAKMAN's private parts, and she felt his private parts on her butt.

29. Another incident Jane Doe 3 described was when they were at the house, and it was morning. Jane Doe 3 was in SPEAKMAN's room, and she was laying on top of SPEAKMAN. There were two (2) other foster children who were in the living room. Jane Doe 3 states after the touching she felt awkward around SPEAKMAN and tried to avoid him. Jane Doe 3 could not recall if SPEAKMAN touched her during this incident but when he previously touched her, he put his hand under her underwear and he would rub her vagina.

30. Jane Doe 3 expressed she was exposed to private parts when she was younger when her mother would bring men home. Jane Doe 3 also stated there was some touching and other things that made her uncomfortable with other minors during the time she lived with SPEAKMAN.

31. On September 15, 2023, the affiant conducted an interview with SPEAKMAN who consented to the interview. SPEAKMAN stated he never touched Jane Doe 3 in an inappropriate manner, and he only touched her as a grandfather should and he loved her. During the interview SPEAKMAN disclosed his Snapchat account was "speakman24."

32. On December 17, 2024, a ICAC database search was conducted on SPEAKMAN with no results.

TECHNICAL BACKGROUND

33. Agents know that, as of January 2024, it is estimated that 97% of American adults possess a cellular phone, and the substantial majority (90%) possess a "smartphone" (a phone capable of, inter alia, connecting to the Internet and downloading mobile applications).[2]

[2] http://www.pewinternet.org/fact-sheet/mobile/

34. Investigative agents also know, through training and experience, that criminals frequently use devices to communicate, including to coordinate and promote criminal acts. These communications can be in the form of calls, text messages or messaging applications built into the social media platforms including photographs, or videos. These communications can be used to make logistical arrangements for criminal act, such as arranging transportation, or disposing of evidence. Device applications may also record the actual physical locations of criminals while planning, or committing crimes. Criminals may also preserve photographs, video or audio of criminal acts. Furthermore, accounts often retain additional information, including use identifiers, contact lists, phone numbers, email accounts or links to other social media accounts which can identify subject, witnesses, and/or the location of additional evidence.

CONCLUSION

35. Based on the above statements it appears there is probable cause to believe that evidence of the violation of 18 U.S.C. § 2251 – Sexual Exploitation of Children will be located at the Subject Premises.

36. Based on the information identified during the investigation regarding SAKIESTEWA and SPEAKMAN there appears to be probable cause to search the Subject Premises. Based on SAKIESTEWA's statements during his interview with the Pueblo of Laguna Police Department and the lack of evidence identified on SAKIESTEWA's phone it is necessary to either include or exclude SPEAKMAN from the investigation regarding the sexual exploitation of children. Since additional electronic devices were identified to be located at SPEAKMAN's residence it would not be out of the realm of possibility for SPEAKMAN and/or SAKIESTEWA to use additional electronic devices to elicit and store the sexual material.

37. The facts outlining that the Target Account was created at the Subject Premises,

the Target Account was created with an email address with the same name as SAKIESTEWA, and the Target Account was used to solicit a nude photo from Jane Doe 1 establishes reasonableness that the offender resides or resided at the Subject Premises. There is also probable cause to believe the photograph in question or other evidence leading to the discovery of who solicited the photograph or where it may have been transferred to can be located at the Subject Premises. Due to the fact that SAKIESTEWA moved from the Subject Premises does not diminish the probable cause to search said location. SPEAKMAN is under investigation for possible sexual abuse of a minor and the information received from the K'awaika Hanu Internet company indicated there was a desktop computer and another unknown electronic device attached to the IP address for SPEAKMAN's residence. This establishes probable cause to believe there is at least one internet capable device at the Subject Premises since SPEAKMAN maintains an internet service there.

38. During the investigation the telephone that was collected from SAKIESTEWA was reasonably excluded as the device that was used to solicit the photograph in question. This opens the possibility that the Target Account was created and managed from another electronic device such as a desktop computer. Based on the information that SAKIESTEWA moved to the secondary address there is also probable cause to search the Subject Premises for any electronic devices that are or were in the possession or control of either SPEAKMAN or SAKIESTEWA.

39. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41. The facts set forth in the previous section show that there are reasonable grounds to believe that the evidence of these offenses, more fully described in Attachment B of this Application, are located in the Subject Premises, described further in Attachment A of this Application. Your affiant respectfully requests this Court issue a search warrant for the Subject Premises,

authorizing the seizure and search for the items described in Attachment B.

40. I swear that this information is true and correct to the best of my knowledge. This affidavit has been reviewed by Supervisory Assistant United States Attorney Alexander Flores.

Respectfully submitted,

Barragan, Adam Kyle
Special Agent
Federal Bureau of Investigation

Electronically submitted and telephonically sworn to before me on January 15, 2025:

THE HONORABLE STEVEN YARBROUGH
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF NEW MEXICO

ATTACHMENT A
PREMISES TO BE SEARCHED

1. The Subject Premises is located at 19 Dusty Hill Road, Mesita, NM 87026 and may be described as a single-story residence with several outbuildings. The primary residence has red siding with white framing and a white door. The front of the residence has a small external porch. Photos of the Subject Premises are below:

2. The search of the Subject Premises shall include the entire residence and all outbuilding, trash cans, and storage containers.

3. This warrant authorizes the forensic examination of any electronic devices seized from the Subject Premises, for the purpose of identifying the electronically stored information described in Attachment B.

4. During the execution of this search, law enforcement personnel are also specifically authorized to compel SPEAKMAN, SAKIESTEWA, and/or anyone found at the Subject Premises reasonably believed by law enforcement to be a user of a device found at the premises to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

a. any of the electronic devices found within the Subject Premises, and

b. where the electronic devices are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments, for the purpose of attempting to unlock the electronic devices' security features in order to search the contents as authorized by this warrant.

5. This does not authorize law enforcement personnel to require SPEAKMAN and/or SAKIESTEWA to state or otherwise provide the password or any other means that may be used to unlock or access the electronic devices, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the electronic devices.

ATTACHMENT B

PROPERTY TO BE SEIZED BY THE GOVERNMENT

I. The following materials, which constitute evidence of a crime, contraband, fruits of crime, or property designed or intended to be used, or which is or has been used as the means of committing a criminal offense, namely violation of 18 U.S.C. §§ 2251.

1. Computers or storage media, computer hardware, computer software (including programs to run operating systems), tablets, cellular phones, applications, computer related documentation, computer passwords, encryption keys, video display monitors connected to such devices used to display contraband images, data security devices, other digital storage devices (e.g., DVDs, CDs, thumb drives, tapes, external hard drives, memory cards, removable data storage devices, and peripherals necessary to access such items, that may be, or are used to: connect to the internet; visually display images; display or access websites, chat sites, and email used as a means to commit the violations described above.

2. All data contained on the above listed items including: active and deleted files that may show the distribution of obscene material to minors, child enticement, production, receipt, possession, transportation, storage, and/or distribution of child pornography, or attempts to do so, including metadata about such files, communications with others about child pornography, online enticement, and child sexual exploitation, information which would tend to show chronological and geographic context of events relating to the crimes under investigation, the identity and/or location of the person(s) involved, the state of mind of such persons, and the identity of others in communication with such persons about child pornography or child sexual abuse.

3. All visual depictions (including images, videos, negatives, still photos, video tapes, artists drawings, slides and any type of computer formatted file) which depict a minor engaged in sexual conduct, or the lewd exhibition of genitalia, or posed or candid in a sexual manner, including clothed or partially clothed.

4. All non-sexual photographs of minors who may be the subject of the visual depictions described in paragraph 1 of this attachment, or the victim of other child exploitation offense or attempted offense as described above, and any information, including names, addresses, nicknames, schools, or after-school groups, that may lead to the age or identity of any minor depicted in any visual media seized.

5. Any correspondence with minor children, including correspondence that may be used to identify the child, or demonstrate an effort to groom, meet, or sexually exploit the child.

6. All information regarding the identity of any real or purported victims or potential victims.

7. All copies and originals of envelopes, letters, diaries, ledgers, journals, chats and other correspondence pertaining to the possession, receipt, distribution, production, and/or

reproduction of visual depictions of a person under the age of 18 years engaging in or simulating sexual conduct, or pertaining to other sexual crimes against children.

8. All materials or items which may be sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such materials includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, journals and fantasy writings.

9. All records, documents, invoices, and materials that concern accounts with any Internet or electronic service provider capable of storing or transmitting child pornography, child erotica, or related communications, as well as any and all records relating to the ownership or use of, or access to, computer equipment found in the residence.

10. All documentation and records, showing discussions by any individual or entity concerning: the selling, licensing, manufacturing, marketing, transferring, providing, furnishing, sampling, or examining of documents, records, images, magnetic media or other items incorporating, or purportedly compatible with the producing, sending, receiving, possessing and viewing of child pornographic materials.

11. All records showing the acquisition and/or sale of computer hardware, computer software, or computer documentation that explains or illustrates how to configure or use computer hardware, and communication programs.

12. All documentation related to computer passwords, encryption keys, and other access devices.

13. All computer hardware equipment, connector cables, and corresponding logs (including: central processing units, monitors, modems, routers, keyboards, printers, computer scanner equipment and or video transfer equipment).

14. All computer software stored on hard disks, digital, optical, and magnetic media devices, and floppy disks containing computer programs, including software data files, electronic mail files, instant message files, software programs and files to receive and or transmit photographs, and operating logs and instruction manuals relating to the operation of the computer hardware and software to be searched.

15. All computer related manuals, textbooks, computer print outs, and other documents used to access computers and record information taken from computers.

16. All documents, web history, and communications demonstrating any communication or correspondence with any person or groups of persons supplying, distributing, or trading in child sexual abuse materials, or discussing a sexual interest in minors, including communications with individuals purporting to be under the age of 18.

17. All accounts or records evidencing manufacturing, production, distribution, receiving, possessing, or sales of printed and photographic materials, negatives, film slides, digital

images, motion pictures, video tapes and documents relating to sexual conduct of persons under the age of 18.

18. Articles of personal property tending to establish the identity of person or persons having the dominion and control over the computer equipment, cellular telephone, or digital media.

19. All safes or lock boxes, where diaries, notes, journals, pictures or other evidence of crimes against children may be stored for safekeeping against seizure.

20. All evidence related to all off-site storage units, other residences, safety deposit boxes, etc. where diaries, notes, journals, pictures or other evidence of crimes against children may be stored for safekeeping against seizure.

21. All cellular telephone records to establish ownership of the device or the residence.

22. Attribution evidence, including:

    a. Contents of volatile memory related to computers and other digital communication devices that would tend to show the current and recent use of the computer, use of encryption, use of other communications devices, routes of Internet and other digital communications traffic and passwords, encryption keys or other dynamic details necessary to preserve the true state of running evidence;
    b. Bookmarks, internet history, temporary internet files, .lnk files, cache files, and other items showing how the computer was accessed, who accessed the computer, and/or how the computer was utilized.
    c. Computer software, hardware or digital contents related to the sharing of Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address;
    d. Any and all documents, records, or correspondence pertaining to online accounts created by or belonging to anyone operating any computer equipment seized;
    e. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical,

arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.